Free Questions for SPLK-2003 by certsinside

Shared by Mcfadden on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following can the format block be used for?

Options:

A- To generate arrays for input into other functions.

B- To generate HTML or CSS content for output in email messages, user prompts, or comments.

C- To generate string parameters for automated action blocks.

D- To create text strings that merge state text with dynamic values for input or output.

Answer:

D

Question 2

Question Type: MultipleChoice

Which of the following supported approaches enables Phantom to run on a Windows server?

Options:

A- Install the Phantom RPM in a GNU Cygwin implementation.

B- Run the Phantom OVA as a cloud instance.

C- Install the Phantom RPM file in Windows Subsystem for Linux (WSL).

D- Run the Phantom OVA as a virtual machine.

Answer:

B

Question 3

Question Type: **MultipleChoice**

Which of the following expressions will output debug information to the debug window in the Visual Playbook Editor?

Options:

A- phantom.debug()

B- phantom.exception()

C- phantom.print ()

D- phantom.assert()

Answer:

D

Question 4

Question Type: MultipleChoice

Which of the following can be configured in the ROI Settings?

Options:

A- Analyst hours per month.

B- Time lost.

C- Number of full time employees (FTEs).

D- Annual analyst salary.

Answer:

D

Question 5

Question Type: MultipleChoice

Which of the following will show all artifacts that have the term results in a filePath CEF value?

Options:

A- .../rest/artifact?_filter_cef_filePath_icontain="results"

B- ...rest/artifacts/filePath="%results%"

C- .../result/artifacts/cef/filePath= '%results%"

D- .../result/artifact?_query_cef_filepath_icontains="results

Answer:

D

Question 6

Question Type: MultipleChoice

Which is the primary system requirement that should be increased with heavy usage of the file vault?

Options:

A- Amount of memory.

B- Number of processors.

C- Amount of storage.

D- Bandwidth of network.

Answer:

C

Question 7

Question Type: MultipleChoice

Which of the following is a step when configuring event forwarding from Splunk to Phantom?

Options:

A- Map CIM to CEF fields.

B- Create a Splunk alert that uses the event_forward.py script to send events to Phantom.

C- Map CEF to CIM fields.

D- Create a saved search that generates the JSON for the new container on Phantom.

Answer:

C

Question 8

Question Type: MultipleChoice

What is the main purpose of using a customized workbook?

Options:

A- Workbooks automatically implement a customized processing of events using Python code.

B- Workbooks guide user activity and coordination during event analysis and case operations.

C- Workbooks apply service level agreements (SLAs) to containers and monitor completion status on the ROI dashboard.

D- Workbooks may not be customized; only default workbooks are permitted within Phantom.

Answer:

D